embodied in hardware, software, or a combination of thereof, that is capable of verifying the authorization of a server to provide resources to the client. Examples of intelligent peripherals include smart cards or PCMCIA devices.

Intelligent peripheral 136 of Figure 7 communicates with server system 60 and verifies the authorization of the server system to provide network resources to client system 10 in much the same way that the client system performed these functions in the embodiment disclosed above in reference to Figures 3-6. In effect, intelligent peripheral 136 is an intermediary device that performs the function of verifying the authorization status of server system 60 on behalf of client system 10. Thus, intelligent peripheral 136 can include the functional components to perform the verification that are otherwise described herein as being included in client system 10.

After intelligent peripheral 136 determines that server system 60 is authorized (or not authorized) to provide resources to client system 10, the client system communicates with the intelligent peripheral. The communication between client system 10 and intelligent peripheral 136 informs the client system whether server system 60 is authorized, and further can include verification of the credentials of the intelligent peripheral, itself. Thus, intelligent peripheral 136 can have the functional components to communicate with client system 10, to verify its own authorization, and to verify the authorization of server system 60 that are otherwise described herein as being included in the server system. System enabler module 56 responds to confirmation that server system 60 is authorized by enabling selected functions of client system 10 in a similar manner as described herein in reference to Figures 3-6.

The use of intelligent peripheral 136 can be useful when server system 60 is not immediately accessible, or when client system 10 and server system 60 are not

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

simultaneously available to communicate directly one with another. Intelligent peripheral 136 can be constructed to prevent encryption keys or other sensitive information contained therein from being accessible to persons who might attempt to disassemble the intelligent peripheral and decode the sensitive information. Those skilled in the art, upon learning of the disclosure made herein, will understand how intelligent peripheral 136 can be constructed to prevent unauthorized access of information.

It is noted that intelligent peripheral 136 can be described as being a component of client system 10. Thus, unless otherwise indicated, any description or claim directed to a client system that verifies the authorization of a server system to provide resources encompasses the embodiment wherein an intelligent peripheral included in the client system performs some or all of the communication with the server system.

Figures 8-10 summarize the steps of one embodiment of the methods for verifying that a server system is authorized to provide network resources to a client system. Figure 8 illustrates a method for composing a client message in response to an authorization interrupt. Figure 9 shows a method whereby an authorized server system receives the client message and composes a corresponding service message. Figure 10 illustrates a method for comparing the contents of the service message with the contents of the client message.

In step 140 of Figure 8, the security counter at the client system increments a security count until it reaches or exceeds the value of the expiration count. In step 142, the client system asserts an authorization interrupt, which will disable some or all non-essential functions of the client system after expiration of a grace period, unless the authorization of the server system is first verified. A random number is then generated in step 144 according to the techniques described herein. The client system combines the random number, the security count, and the client identifier to form a client message in step 146. In step 148, the

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

client message is encrypted as described herein. As shown at step 150, the encrypted message is then transmitted to the server system.

Referring to Figure 9, the server system receives the client message in step 152. The server system then decrypts the client message in step 154 and decombines the client message in step 156 as disclosed herein. Using the client identifier, the server system selects an authorization code to be associated with the client system as shown at step 158. The server system also selects a new expiration count in step 160, thereby indicating when the next reauthorization procedure should be initiated. In step 162, the server system combines the random number, the authorization code, and the new expiration count to form a service message. The service message is then encrypted in step 164 and transmitted to the client system in step 166.

As illustrated in Figure 10, the client system receives the service message according to step 168. The client system then decrypts the service message in step 170 and decombines the service message in step 172. As shown at step 174, the client system compares the random number contained in the service message with the original random number contained in the client message. According to decision block 176, if the random numbers are the same, the authorization of the server system to provide network resources to the client system has been verified, and the method advances to step 178, in which the authorization code causes selected functions of the client system to be enabled, whereby selected resources from the server can be received by the client. Next, in step 180, the new expiration count is set, and will cause the method of Figures 8-10 to repeat when the security count again exceeds the expiration count.

If the server system had been unauthorized, any service message generated thereby would not have included the random number. In this case, decision block 176 would be

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111